

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ CVE-2026-89111 ในผลิตภัณฑ์ SAP's Cloud SDK for Python

วันที่แจ้งเตือน 21 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์พบรายงานกรณีช่องโหว่ระดับ Critical ใน SAP's Cloud SDK for Python เสียข้อมูล application's OAuth2 client credentials รั่วไหล

การโจมตี	ผลกระทบ
- Cloud SDK for Python ที่เป็นส่วนต่อประสานสำหรับพัฒนาแอปพลิเคชันที่เชื่อมต่อบริการบน SAP Business Technology Platform (BTP) - ช่องโหว่ดังกล่าว (CVE-2026-89111) เป็นช่องโหว่ประเภท Server-Side Request Forgery (SSRF) เป็นช่องโหว่จากการตรวจสอบค่า tenant_subdomain ไม่เหมาะสม ก่อนนำไปสร้าง URL สำหรับร้องขอ OAuth2 Token ในแอปพลิเคชัน (Multi-tenant application) - ผู้ไม่หวังดีที่สามารถควบคุมค่าดังกล่าวได้ อาจทำให้ระบบส่งข้อมูล application's OAuth2 client credentials ไปยังปลายทางที่ผู้ไม่หวังดีและอาจนำข้อมูลที่ได้รับไปใช้เข้าถึงบริการตามสิทธิของแอปพลิเคชันนั้น ผู้ไม่หวังดีควบคุม Tenant → SAP Cloud SDK ขาดการตรวจสอบค่าที่เหมาะสม → ค่าขอ OAuth2 ถูกส่งไปยัง Server ของผู้ไม่หวังดี → Credentials รั่วไหล	- เนื่องจากช่องโหว่ SDK อาจส่ง application's OAuth2 client credentials ไปยังเซิร์ฟเวอร์ที่ผู้ไม่หวังดีควบคุม ทำให้เกิดความเสี่ยงต่อการรั่วไหลของ credentials และผู้ไม่หวังดีสามารถดำเนินการต่อได้ขึ้นอยู่กับสิทธิของ client นั้น ผลิตภัณฑ์ SAP ที่ได้รับผลกระทบ: SAP Cloud SDK for Python หรือแพ็คเกจ sap-cloud-sdk ในเวอร์ชันต่อไปนี้ - SAP Cloud SDK for Python ต่ำกว่า Version 0.45.2 รวมถึง Version 0.36.1 และ Version 0.36.2 ตามขอบเขตที่ SAP ระบุ - SAP Cloud SDK for Python ตั้งแต่ Version 0.53.0 ถึง 0.55.0 ควรตรวจสอบและอัปเดตเพิ่มเติมเนื่องจากพบข้อผิดพลาดการตรวจสอบค่า tenant subdomain
คำแนะนำ: - ตรวจสอบ Version ของแพ็คเกจ sap-cloud-sdk ในแอปพลิเคชันทุกระบบภายในหน่วยงานรวมถึงระบบทดสอบ, ระบบใช้งานจริง และ Container Image พร้อมตรวจสอบการใช้งานค่า tenant_subdomain - เร่งอัปเดต SAP Cloud SDK for Python เป็นรุ่นที่ได้รับการแก้ไข ดังนี้ - สำหรับ Version 0.45.2 ลงมา ให้อัปเดตเป็น version 0.45.2 หรือพิจารณา version 0.55.1 หลังทดสอบความเข้ากันได้ - สำหรับ version 0.53.0 ถึง 0.55.0 ให้อัปเดตเป็น version 0.55.1 - สำหรับ version ใหม่กว่า ควรตรวจสอบ Release Notes และความเข้ากันได้ - ปรับปรุงไฟล์กำหนด Dependencies และ Lock File พร้อม Build และนำแอปพลิเคชันขึ้นใช้งานใหม่ เพื่อให้ระบบที่ทำงานอยู่ใช้แพ็คเกจที่ได้รับการแก้ไข	- สำรองค่าการตั้งค่าที่สำคัญและเตรียมแผนกู้คืนบริการก่อนอัปเดต พร้อมทดสอบการร้องขอToken และการเชื่อมต่อบริการ SAP BTP ที่แอปพลิเคชันใช้งาน - หลังอัปเดตให้ตรวจสอบหมายเลขเวอร์ชันในระบบที่ใช้งานจริงและทดสอบว่าระบบปฏิเสธค่า tenant_subdomain ที่ไม่ถูกต้องโดยใช้ข้อมูลทดสอบ แทนการใช้ credentials จริง - ตรวจสอบ Log ของแอปพลิเคชันและการเชื่อมต่อขาออก เพื่อค้นหาการร้องขอToken ไปยังโดเมนที่ไม่รู้จัก หรือค่า tenant_subdomain ที่ไม่ตรงกับองค์กรผู้ใช้งานที่ลงทะเบียนไว้ - หากพบหรือสงสัยว่า Client Secret รั่วไหล ให้เปลี่ยนข้อมูล credentials ที่เกี่ยวข้อง ตรวจสอบการใช้งานย้อนหลัง และพิจารณาเพิกถอน Token ตามความสามารถของบริการ พร้อมดำเนินการตามกระบวนการตอบสนองเหตุการณ์
แนวทางลดความเสี่ยงชั่วคราว: - Allowlist Tenant: ตรวจสอบ tenant_subdomain กับรายการองค์กรที่ได้รับอนุญาตก่อนส่ง SDK - จำกัดการเชื่อมต่อเฉพาะ OAuth2 และบริการที่จำเป็น และ ทบทวนสิทธิ แยก Credentials ระหว่าง Test/Production	- Monitoring: เฝ้าระวัง Token Request ที่ผิดปกติ และไม่บันทึก Client Secret/Access Token ใน Log - Incident Response: หากพบความผิดปกติ ให้เก็บหลักฐาน จำกัดการเชื่อมต่อที่ต้องสงสัย และเข้าสู่กระบวนการตรวจสอบเหตุการณ์ทันที

ข้อมูลอ้างอิง

- รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 20 ต.ค. 2569
- <https://thehackernews.com/2026/10/sap-discloses-critical-cvss-10-flaw-in.html?>

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ CVE-2026-76268, CVE-2026-76281 และ CVE-2026-76284 ในผลิตภัณฑ์ Splunk Enterprise

วันที่แจ้งเตือน 21 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์พบรายงานกรณีช่องโหว่หลายรายการในซอฟต์แวร์ Splunk Enterprise โดยช่องโหว่ดังกล่าวทำให้ผู้ไม่หวังดีสามารถยกระดับสิทธิ์ (Privilege Escalation) สั่งรันคำสั่งบนระบบปฏิบัติการ และเข้ายึดครองระบบของหน่วยงานได้

การโจมตี	ผลกระทบ
- CVE-2026-76268 เกิดจากความบกพร่องในการยืนยันตัวตน ส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงเครือข่ายของ Patroni REST API และสามารถรันคำสั่งของระบบปฏิบัติการได้ตามต้องการ - CVE-2026-76281 เกิดจากการควบคุมการเข้าถึงที่ไม่เหมาะสม (Improper Access Control) ทำให้ผู้ไม่หวังดีสามารถเรียกใช้งานฟังก์ชันระดับผู้ดูแลระบบได้โดยไม่ต้องใช้ Credentials ที่ถูกต้อง และอาจเข้าควบคุมฟังก์ชันของระบบที่ถูกจำกัดสิทธิ์ไว้ได้ - CVE-2026-76284 เกิดจากช่องโหว่การจัดการและคัดกรองข้อมูล ทำให้ผู้ไม่หวังดีสามารถแทรกข้อมูลหรือรันคำสั่งที่เป็นอันตรายเข้าสู่ระบบ และสามารถยึดระบบ หรือแก้ไขเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต	ผลิตภัณฑ์ที่ได้รับผลกระทบ: Splunk Enterprise Versions 10.4.0 - 10.4.2 Splunk Enterprise Versions 10.2.0 - 10.2.6 Splunk Enterprise Versions 10.0.0 - 10.0.9 Splunk Enterprise Versions 9.4.0 - 9.4.14
คำแนะนำ: - ตรวจสอบและอัปเดต เป็นเวอร์ชันล่าสุดทันที - จำกัดสิทธิ์การเข้าถึงเครือข่าย ตั้งค่าอนุญาตให้เฉพาะผู้ดูแลระบบหรืออุปกรณ์ที่ระบุเท่านั้นที่สามารถเชื่อมต่อเข้าถึง Patroni REST API และพอร์ตจัดการระบบของ Splunk เพื่อป้องกันการโจมตีจากบุคคลภายนอก - ตรวจสอบประวัติการล็อกอินด้วยสิทธิ์ผู้ดูแลระบบ การแก้ไขการตั้งค่าที่สำคัญ หรือคำสั่งแปลกปลอมในระบบ เพื่อดูว่ามีร่องรอยการถูกเจาะระบบหรือไม่ หากพบความผิดปกติ ให้รีบตัดการเชื่อมต่อระบบออกจากเครือข่ายทันที	

ข้อมูลอ้างอิง

- รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 20 ต.ค. 2569
- <https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-145/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

ช่องโหว่ Vghost (CVE-2026-74580) ใน Linux Kernel

วันที่แจ้งเตือน 21 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพ์และผู้ประกอบธุรกิจสินทรัพ์ดิจิทัล

ThaiCERT สกมช. ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์พบรายงานกรณีช่องโหว่ Vghost ใน Linux Kernel เสี่ยงต่อผู้ไม่หวังดีสามารถยกระดับสิทธิเป็น root และอาจเข้ายึดเครื่องแม่ข่ายผ่าน Virtual Machine ได้

การโจมตี	ผลกระทบ
- ช่องโหว่ Vghost ในโมดูล vhost ของ Linux Kernel ซึ่งเป็นโมดูลสำหรับเพิ่มประสิทธิภาพการรับส่งข้อมูล (I/O) ของเครื่องเสมือน (Virtual Machine) - สาเหตุจากข้อผิดพลาดในการจัดการหน่วยความจำ (Memory Corruption) ทำให้ระบบอ่านหรือเขียนข้อมูลในตำแหน่งหน่วยความจำที่ไม่ถูกต้อง โดยอาจส่งผลกระทบต่อระบบใน 2 ลักษณะ ดังนี้ - การยกระดับสิทธิ (Privilege Escalation) ผู้ไม่หวังดีสามารถใช้งาน vhost ที่ได้รับผลกระทบเพื่อเข้าถึงหน่วยความจำของ Kernel และยกระดับสิทธิเป็น root ของระบบ Linux ได้ - การโจมตีข้ามเครื่องเสมือน (VM Escape) โดยผู้ไม่หวังดีที่สามารถเข้าควบคุมเครื่องเสมือน (Guest VM) อาจใช้ประโยชน์จากช่องโหว่เพื่อโจมตีข้ามไปยังเครื่องแม่ข่าย (Host) และเข้าควบคุม QEMU process บนเครื่อง Host เพื่อเข้าถึงข้อมูลหรือควบคุมทรัพยากร	- ผู้ไม่หวังดีสามารถยกระดับสิทธิเป็น root ได้ทันที ซึ่งทำให้สามารถควบคุมระบบทั้งหมดได้ รวมถึงการติดตั้งมัลแวร์, ขโมยข้อมูล, หรือทำลายระบบ - กรณี Virtualization ผู้ไม่หวังดีใน Guest VM สามารถเข้าไปควบคุม Host ได้ (Guest-to-Host Escape) ซึ่งถือเป็นภัยคุกคามร้ายแรงต่อโครงสร้างพื้นฐานคลาวด์และเซิร์ฟเวอร์เสมือน เนื่องจากสามารถเข้าถึงข้อมูลและทรัพยากรของ Host และ Guest อื่นๆ ที่รันอยู่บน Host เดียวกันได้ ผลิตภัณฑ์ที่ได้รับผลกระทบ: - ระบบปฏิบัติการ Linux Kernel ที่ใช้งานโมดูล vhost - อุปกรณ์หรือเซิร์ฟเวอร์ที่ติดตั้ง Ubuntu , RHEL, Amazon Linux, Microsoft Azure Linux, และ Oracle Linux ที่ยังไม่ได้รับการแพตช์ - สภาพแวดล้อม Virtualization ที่ใช้งาน QEMU/KVM ร่วมกับ vhost-net หรือ vhost-vsock โดยเฉพาะเมื่อเปิดใช้งาน virtual IOMMU และ device-IOTLB mode
คำแนะนำ: - ตรวจสอบเวอร์ชัน Linux Kernel ที่ใช้งานอยู่ หากเป็นเวอร์ชันที่ได้รับผลกระทบตั้งแต่ 4.11 ถึง 7.2-rc4 ให้ดำเนินการอัปเดตเป็นเวอร์ชันที่ได้รับการแก้ไขแล้ว โดยตรวจสอบรายละเอียดได้ที่ https://dg.th/207pc3ayis - สำหรับ Ubuntu ให้ตรวจสอบสถานะการแก้ไขช่องโหว่ของเวอร์ชัน 24.04 และ 26.04 และดำเนินการติดตั้งแพตช์ตามคำแนะนำของผู้พัฒนา https://dg.th/p6x6uwn8yc7 - สำหรับ Red Hat Enterprise Linux ให้ตรวจสอบสถานะการแก้ไขช่องโหว่และติดตั้งแพตช์ https://dg.th/jzgov0fwsl	- สำหรับ Amazon Linux ให้ตรวจสอบสถานะการแก้ไขช่องโหว่และติดตั้งแพตช์ https://dg.th/hoj05klzq9 - สำหรับ Oracle Linux ให้ตรวจสอบสถานะการแก้ไขช่องโหว่และติดตั้งแพตช์ https://dg.th/86k5v7gqp2 - ตรวจสอบสิทธิการเข้าถึง device nodes /dev/vhost-net และ /dev/vhost-vsock ว่ามีสิทธิ world-readable (mode 0666) หรือไม่ หากมี ให้จำกัดสิทธิทันที - ตรวจสอบว่าระบบมีการใช้งาน virtual IOMMU และ device-IOTLB mode หรือไม่ หากมีการใช้งานในสภาพแวดล้อมที่ไว้วางใจ Guest ไม่เพียงพอ ให้พิจารณาปิดการใช้งานฟีเจอร์ดังกล่าวชั่วคราวจนกว่าจะอัปเดต Kernel
แนวทางลดความเสี่ยงชั่วคราว: - จำกัดการเข้าถึง device nodes /dev/vhost-net และ /dev/vhost-vsock โดยลบสิทธิ world access และจำกัดกลุ่มผู้ครอบครอง (owning group) ให้เฉพาะบริการ virtualization ที่ไว้วางใจเท่านั้น - พิจารณาการปิดใช้งาน vhost-net หรือ vhost-vsock ชั่วคราว หากไม่จำเป็นสำหรับการใช้งานในระหว่างที่ยังไม่สามารถอัปเดต Kernel ได้ - สำหรับสภาพแวดล้อม Virtualization ที่ไม่สามารถอัปเดต Host Kernel ได้ทันที ให้พิจารณาการแยก Guest VM ออกจาก Host หรือใช้มาตรการควบคุมการเข้าถึงเครือข่ายภายใน Guest เพื่อลดโอกาสการโจมตีข้ามขอบเขต	

ข้อมูลอ้างอิง

1.

รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 20 ต.ค. 2569
2.

<https://thehackernews.com/2026/10/ai-found-linux-kernel-flaw-gives-local.html>